MATHEMATICS

SOME THEOREMS ON UNIVERSAL ALGEBRAS. I

BY

PH. DWINGER

(Communicated by Prof. H. D. KLOOSTERMAN at the meeting of October 27, 1956)

It is well-known that the congruence relations of a universal (general abstract) algebra form a complete modular lattice if any two of the congruence relations of the algebra are permutable. We mention the following algebras as belonging to this class: groups [3], finite loops and a certain class of infinite loops [3], [13], finite quasi-groups [11], finite distributive lattices [10], relatively complemented lattices [5], complemented modular lattices and thus Boolean algebras. The main part of the present paper is devoted to the proof of a general theorem on finite and infinite direct unions of algebras all of whose congruence relations are permutable and with a selected one-element subalgebra. For the proof of this theorem we shall use the results obtained in a previous paper [6] on complete modular lattices which satisfy an axiom introduced by BAER [1]. Furthermore we shall prove some theorems on the group of automorphisms of an algebra and a certain subgroup of the group of automorphisms of the lattice of congruence relations of the algebra.

1. *Some preliminary remarks on modular lattices*

Throughout this paper L always stands for a complete modular lattice, the zero and unit element of which are denoted by 0 and 1 respectively. Small characters always denote elements of L. If $a \leqslant b$ then $[a, b]$ denotes the interval consisting of all elements x, $a \leqslant x \leqslant b$.

The modular law is given by

$$a+bc=(a+b)c \text{ for any three elements } a, b \text{ and } c,\ a \leqslant c \tag{A}$$

If $\{x_\alpha\}$ is a set of elements of L, where α ranges over an index set A then the sum and the product of $\{x_\alpha\}$ are denoted by $\sum\limits_{\alpha \in A} x_\alpha$ and $\prod\limits_{\alpha \in A} x_\alpha$ respectively. An element a is the *direct sum* of the elements x and x', $a = x \oplus x'$ if $a = x + x'$ and $0 = xx'$. Dually, an element a is the *direct product* of the elements x and x', $a = x \otimes x'$ if $a = xx'$ and $1 = x + x'$. x is a *direct summand* of a if there exists an element x' such that $a = x \oplus x'$. The concept *direct factor* of a is defined dually. The element a is the direct sum of a set of elements $\{x_\alpha\}$, $\alpha \in A$, $a = \sum\limits_{\alpha \in A}{}^* x_\alpha$ if for every $\alpha \in A$, $a = x_\alpha \oplus x'_\alpha$ where $x'_\alpha = \sum\limits_{\substack{\beta \in A \\ \beta \neq \alpha}} x_\beta$. We say that $a = \sum\limits_{\alpha \in A}{}^* x_\alpha$ is a decomposition of a into direct summands. Dually, a is the direct product of $\{x_\alpha\}$, $\alpha \in A$, $a = \prod_{\alpha \in A} {}^* x_\alpha$ if for every $\alpha \in A$, $a = x_\alpha \otimes x_\alpha^*$ where $x_\alpha^* = \prod_{\substack{\in A \\ \beta \neq \alpha}} x_\beta$. Again we say that $a = \prod_{\alpha \in A} {}^* x_\alpha$ is a decomposition of a into direct factors. If we talk about a direct decomposition of a we always mean a decomposition into direct summands of a. If the set $\{x_\alpha\}$ consists of only one element then we say that this element is the direct sum and also the direct product of the set. An element a is called *minimal* if $a \neq 0$ and $a \geqslant x > 0$ implies $x = a$, *indecomposable* if its only direct summands are 0 and a, *decomposable* if it has a direct summand not 0 and not a, *completely decomposable* if it is the direct sum of indecomposable elements and *completely reducible* if it is the direct sum of a *finite* number of minimal elements. A direct summand x of a is called a *proper summand* of a if $x \neq 0$. A complete lattice L, not necessarily modular, satisfies the axiom of Baer [1] if for each system of elements y, z, $\{x_\alpha\}$, $\alpha \in A$ satisfying the condition $y < z \leqslant \sum_{\alpha \in A} x_\alpha$, there is a finite number of x_α, say $x_1, x_2, \ldots, x_n$, such that

$$y(x_1 + x_2 + \ldots + x_n) < z(x_1 + x_2 + \ldots + x_n) \tag{B}$$

Remark. Baer has introduced this axiom in order to develop the theory on infinite direct products in complete modular lattices. However we observe that Kurosh [9] has introduced an other axiom which can be considered as a generalisation of the modular law to the infinite case and which also can serve for the development of the theory of infinite direct sums. The author and J. de Groot [7] have proved that in case of modular lattices the axiom of Kurosh is weaker than the axiom of Baer. In the present paper we shall make use of the axiom of Baer since we need some results on infinite products for the proof of which the validity of the axiom of Baer is required [6]. In connection with this, we note that in the applications of our results, the lattices which we shall consider always satisfy the axiom of Baer (and thus, if they are modular, the axiom of Kurosh).

For the theory of direct decompositions in complete modular lattices we refer the reader to [9] and [6]. The theory of direct products is developed in [6]. We quote from [6] the following theorems which we shall need in particular. For the proofs we refer to [6]

Theorem 1.1 (Lemma 3 in [6])

If a complete modular lattice L satisfies the axiom of Baer and $\{x_\alpha\}$, $\alpha \in A$ is a set of elements of L, *and* $\sum_{\alpha \in A} x^\alpha = \sum_{\alpha \in A}^* x^\alpha$, then for every $A_1 \subset A$ we have

$$\prod_{\alpha \in A_1} x'_\alpha = \sum_{\alpha \in A_1'}^* x_\alpha$$

where A_1' means the set-theoretic complement of A_1 in A and $x'_\alpha = \sum_{\substack{\beta \in A \\ \beta \neq \alpha}} x_\beta$

Theorem 1.2 (Theorem 3 in [6])

If a complete modular lattice L satisfies the axiom of Baer and $\{x_\alpha\}$, $\alpha \in A$ is a set of elements of L for which $\sum_{\alpha \in A} {}^* x_\alpha = 1$ then we have

$$\prod_{\alpha \in A} x'_\alpha = \prod_{\alpha \in A}{}^* x'_\alpha = 0.$$

Theorem 1.3 (Theorem 4 in [6])

If $\{x_\alpha\}$, $\alpha \in A$ is a *finite* set of elements of a complete modular lattice L for which $\prod_{\alpha \in A} {}^* x_\alpha = 0$ then we have

(i) $x_\alpha = \sum_{\substack{\beta \in A \\ \beta \neq \alpha}} x^*_\beta$ for every $\alpha \in A$, hence $x_\alpha = (x^*_\alpha)'$.

(ii) $\sum_{\alpha \in A} x^*_\alpha = \sum_{\alpha \in A}{}^* x^*_\alpha = 1.$

Finally we whall need the following lemma.

Lemma 1.1

Any indecomposable element in a complemented lattice is minimal.

Proof.

If a modular lattice is complemented then it is relatively complemented ([3], p. 114).Thus if x is indecomposable but not minimal then there exists an element x', $0 < x' < x$ and thus there is an element x'', such that $x' \oplus x'' = x$ contradicting that x is indecomposable.

Chains in modular lattices

An ordered finite system of elements $0 = x_0 < x_1 < \ldots < x_n = 1$ is called a *normal* chain, the length of which is n, with the factors $[x_k, x_{k+1}]$ A *principal* chain is a normal maximal chain. A modular lattice satisfies the *ascending (descending) chain condition* if all its ascending (descending) chains are finite. If L satisfies either chain condition then we say that L has finite length. Two intervals of L which can be written as $[xy, x]$ and $[y, x+y]$ are called *transposes*. Two intervals $[x, y]$ and $[x'. y']$ are called *projective*, if there is a finite sequence of intervals

$$[x, y],\ [x_1, y_1],\ [x_2, y_2],\ \ldots,\ [x', y'],$$

in which any two successive intervals are transposes. Two normal chains are isomorphic if their lengths are equal and if there exists a one-one correspondence between their elements, such that the corresponding factors are projective (see Lemma 1.2 below). For the proofs of the following Lemma 1.2 and the Theorems 1.4 and 1.5 we refer the reader to [3].

Lemma 1.2

Projective intervals are isomorphic in any modular lattice.

Theorem 1.4 (Theorem of Jordan–Hölder)
Any two principal chains in a modular lattice are isomorphic.

Theorem 1.5 (Theorem of Schreier–Zassenhaus)
Any two normal chains in a modular lattice have isomorphic refinements.

Theorem 1.6
If L has a principal chain, then the length of every normal chain is at most the length of a principal chain.

The proof follows immediately from the preceding theorems. From Theorem 1.6 we infer the following theorem.

Theorem 1.7
L has a principal chain if and only if L has finite length.

§ 2. *Universal or general abstract algebras*

We use the term (universal or general abstract) algebra in the sense of BIRKHOFF [3].

An algebra $\mathfrak{A}$ is a set of elements together with a set of operations f_α, where every f_α is a single valued function assigning to every sequence $(x_1, x_2, \dots, x_n)$, every $x_i \in \mathfrak{A}$, n finite and $n=n(\alpha)$, an element

$$f_\alpha(x_1, x_2, \dots, x_n) \in \mathfrak{A}.$$

Subalgebra, isomorphism, homomorphism and endomorphism have the usual meaning. The direct union of a finite set of algebras

$$\mathfrak{A}_1, \mathfrak{A}_2, \dots, \dots, \mathfrak{A}_n,$$

having the same operations is denoted by $\mathfrak{A}_1 \times \mathfrak{A}_2 \times \dots \times \mathfrak{A}_n$ and defined in the usual way. Thus if

$$\mathfrak{A} = \mathfrak{A}_1 \times \mathfrak{A}_2 \text{ and } (x_i, y_i) \in \mathfrak{A},\ x_i \in \mathfrak{A}_1, y_i \in \mathfrak{A}_2,\ i=1, 2, \dots, n$$

then

$$f_\alpha((x_1, y_1), (x_2, y_2), \dots, (x_n, y_n)) = (f_\alpha(x_1, x_2, \dots, x_n), f_\alpha(y_1, y_2, \dots, y_n))$$

A *congruence relation* θ of an algebra $\mathfrak{A}$ is an equivalence relation with the substitution property for every f_α. Thus if

$$x_i \equiv y_i (\mathrm{mod}\ \theta), \quad i=1, 2, \dots, n$$

then

$$f_\alpha(x_1, x_2, \dots, x_n) \equiv f_\alpha(y_1, y_2, \dots, y_n)\ (\mathrm{mod}\ \theta) \text{ for every } f_\alpha.$$

It is clear that every congruence relation θ defines a homomorphic mapping θ^* of $\mathfrak{A}$ onto the algebra of the residue classes of $\mathfrak{A}$ modulo θ. This algebra is denoted by $\mathfrak{A}/_\theta$ or $\mathfrak{A}_\theta$ or $(\mathfrak{A})_\theta$. The image of an element $x \in \mathfrak{A}$ under the mapping θ^* is denoted by $x^{\theta *}$. Conversely every homomorphic mapping λ of an algebra $\mathfrak{A}$ onto an algebra $\mathfrak{A}'$ defines a congruence relation θ of $\mathfrak{A}$ by $x \equiv y (\mathrm{mod}\ \theta)$ if and only if $x^\lambda = y^\lambda$. If θ is a congruence relation of $\mathfrak{A}$ and $a \in \mathfrak{A}$, then $S_a(\theta)$ denotes the set of all elements $x \in \mathfrak{A}$, for which $x \equiv a(\text{mod}\,\theta)$. If $\mathfrak{A}$ has a selected one-element subalgebra 1, then we write $S(\theta)$ instead of $S_1(\theta)$. It is not difficult to show that $S(\theta)$ is a subalgebra of $\mathfrak{A}$. If $\mathfrak{A}'$ is a subalgebra of $\mathfrak{A}$ and θ some congruence relation of $\mathfrak{A}$ then θ induces in $\mathfrak{A}'$ a congruence relation θ', defined by $x \equiv y\,(\text{mod}\,\theta')$ if and only if $x \equiv y(\text{mod}\,\theta)$, x and $y \in \mathfrak{A}'$. However if there is no danger for confusion we write θ instead of θ'. It is not difficult to prove [3] that the set $C[\mathfrak{A}]$ of all congruence relations of an algebra $\mathfrak{A}$ can be made into a complete lattice by defining $\theta_1 \leqslant \theta_2$ if and only if $x \equiv y(\text{mod}\,\theta_1)$ implies $x \equiv y(\text{mod}\,\theta_2)$ for every x and $y \in \mathfrak{A}$. Then the sum and the product of a set $\{\theta_\alpha\}$, $\alpha \in A$ of congruence relation are given by $x \equiv y(\text{mod} \sum_{\alpha \in A} \theta_\alpha)$ if there exists a sequence of elements in $\mathfrak{A}$,

$$x = z_1, z_2, \ldots, z_i, z_{i+1}, \ldots, z_n = y \text{ such that } z_{i-1} \equiv z_\iota(\text{mod}\,\theta_{\alpha_\iota})$$

for some $\alpha_\iota \in A$ and for $\iota = 1, 2, \ldots, n-1$ and

$$x \equiv y(\text{mod} \prod_{\alpha \in A} \theta_\alpha) \text{ if } x \equiv y(\text{mod}\,\theta_\alpha) \text{ for every } \alpha \in A.$$

The zero and unit element of $C[\mathfrak{A}]$ will be denoted by 0 and 1 respectively. Thus $x \equiv y(\text{mod}\,0)$ implies $x = y$ and $x \equiv y(\text{mod}\,1)$ for any x and $y \in \mathfrak{A}$. If $\mathfrak{A}$ has a selected one-element subalgebra, then we shall also denote this element by 1 since there will not arise any danger for confusion. If $\mathfrak{A}$ has a one-element subalgebra then it is obvious that for any pair of congruence relations θ and φ we have $\varphi' = (\theta\varphi)'$, where φ' and $(\theta\varphi)'$ are the congruence relations induced by φ and $\theta\varphi$ in $S(\theta)$. Furthermore if $\theta' \geqslant \theta$ then instead of $S(\theta')/\theta$ we also write θ'/θ [3]. Finally we note that instead of $x \equiv y(\text{mod}\,\theta)$, we shall also write $x\theta y$. Thus $x\theta_1 y\theta_2 z$ means $x \equiv y(\text{mod}\,\theta_1)$ and $y \equiv z(\text{mod}\,\theta_2)$.

§3. *Permutable congruence relations*

Two congruence relations of an algebra $\mathfrak{A}$, θ_1 and θ_2 are *permutable* if the following condition is satisfied: whenever $x \equiv z(\text{mod}\,\theta_1)$ and $z \equiv y(\text{mod}\,\theta_2)$, x, y and $z \in \mathfrak{A}$, then there exists a $z' \in \mathfrak{A}$ such that

$$x \equiv z'(\text{mod}\,\theta_2) \text{ and } z' \equiv y(\text{mod}\,\theta_1).$$

It is clear that the relation of permuability is symmetric and reflexive but need not be transitive. Furthermore it is not difficult to prove that if θ_1 and θ_2 are permutable, we have $x \equiv y(\text{mod}\,(\theta_1 + \theta_2))$ if and only if there exists an element z such that $x\theta_1 z\theta_2 y$. [3].

It follows from an elementary group-theoretic argument, that the congruence relations of an (operator) group are permutable. We note that the lattice of congruence relations of an (operator) group is isomorphic with the lattice of (admissable) normal subgroups ordered under setinclusion. BIRKHOFF [3] has shown that the congruence relations of a finite loop are permutable and has given a sufficient condition in order that any two congruence relations of a loop are permutable. Recently COWELL [3]1 has weakened this condition. On the other hand GOLDIE [8] has proved that the congruence relations of a loop which are generated by its normal subloops are permutable. Other exemples of algebras, any two congruence relations of which are permutable, are finite quasigroups (WANG, [11]), finite distributive lattices (THURSTON, [10]) relatively complemented lattices (DILWORTH, [5]) and thus complemented modular lattices, since every complemented modular lattice is relatively complemented. In particular the congruence relations of any Boolean algebra are permutable.

Theorem 3.1

If $\mathfrak{A}$ is an algebra any two congruence relations are permutable, then $C[\mathfrak{A}]$ is a modular lattice (BIRKHOFF, [3]).

Proof

If $\theta_1 \leqslant \theta_3$ and $x(\theta_1+\theta_2)\theta_3 y$ then $x\theta_1 z\theta_2 y, x\theta_3 y$ for some $z \in \mathfrak{A}$. Thus

$$x(\theta_1+\theta_2\theta_3)y \text{ and thus } (\theta_1+\theta_2)\theta_3 \leqslant \theta_1+\theta_2\theta_3.$$

Obviously

$$\theta_1+\theta_2\theta_3 \leqslant (\theta_1+\theta_2)\theta_3 \text{ and thus } \theta_1+\theta_2\theta_3 = (\theta_1+\theta_2)\theta_3.$$

Theorem 3.2

The lattice of congruence relations of *any* algebra satisfies the postulate (B) of Baer.

Proof

Suppose $\varphi < \psi \leqslant \sum_{\alpha \in A} \theta_\alpha$, $\alpha \in A$ for some system of congruence relations φ, ψ and $\{\theta_\alpha\}$, $\alpha \in A$. If (B) would not hold, then for every finite set of indices $\alpha_1, \alpha_2, \ldots, \alpha_n$, every $\alpha_i \in A$, we would have

$$\varphi(\theta_{\alpha_1}+\theta_{\alpha_2}+\ldots+\theta_{\alpha_n}) = \psi(\theta_{\alpha_1}+\theta_{\alpha_2}+\ldots+\theta_{\alpha_n}).$$

Now if $x\psi y$ then $x(\sum_{\alpha \in A} \theta_\alpha)y$ and thus there exists a finite set of indices $\alpha_1, \alpha_2, \ldots, \alpha_n$, every $\alpha_i \in A$ such that

$$x(\theta_{\alpha_1}+\theta_{\alpha_2}+\ldots+\theta_{\alpha_n})y \text{ and thus } x\psi(\theta_{\alpha_1}+\theta_{\alpha_2}+\ldots+\theta_{\alpha_n})y.$$

But then

$$x\varphi(\theta_{\alpha_1}+\theta_{\alpha_2}+\ldots+\theta_{\alpha_n})y \text{ and thus } x\varphi y.$$

From this it would follow $\psi \leqslant \varphi$ contradicting $\varphi < \psi$ completing the proof.

If two congruence relations of $\mathfrak{A}$ are permutable, then they need not induce in a subalgebra of $\mathfrak{A}$ premutable congruence relations again. However we can state the following lemma.

Lemma 3.1

If θ, θ_1 and θ_2 are congruence relations of $\mathfrak{A}$ and $\mathfrak{A}$ has a selected one-element subalgebra 1 and $\theta_1 \leqslant \theta$ and θ_1 and θ_2 are permutable, then θ_1' and θ_2' are permutable in $S(\theta)$.

Proof

If $x\theta_1'z\theta_2'y$ for some $z\theta 1$, then $x\theta_1 z\theta_2 y$ and thus $x\theta_2 z'\theta_1 y$ for some $z' \in \mathfrak{A}$. But $\theta_1 \leqslant \theta$ thus $z'\theta y\theta 1$ which implies $z'\theta 1$ completing the proof.

§ 4. *Isomorphism Theorems and Lemma of Zassenhaus*

The isomorphism theorems have already been formulated for general algebras by several authors (BOURBAKI [4], BIRKHOFF [3], GOLDIE [8]). Following Birkhoff we shall give in this section a lattice-theoretic formulation with a view of the applications in the following sections. Goldie has given a formulation of the Lemma of Zassenhaus for general algebras. We shall give a simple lattice-theoretic proof in case of algebras with permutable congruence relations. Finally we shall prove in this section some theorems concerning homomorphic mappings of algebras.

We recall that if $a \in \mathfrak{A}$ and $\theta \in C[\mathfrak{A}]$ that $S_\alpha(\theta)$ denotes the set of all $x \in \mathfrak{A}$ for which $x\theta a$. Furthermore if θ_1 and θ_2 are two congruence relations of $\mathfrak{A}$ then $S(\theta_2 \cdot \theta_1)$ denotes the set of all elements $x \in \mathfrak{A}$ for which $x\theta_2 z\theta_1 a$ for some $z \in \mathfrak{A}$.

Lemma 4.1

If $S_a(\theta)$ is a subalgebra of $\mathfrak{A}$ for some $a \in \mathfrak{A}$ and some $\theta \in C[\mathfrak{A}]$ then $S_a(\theta_1 \cdot \theta)$ is a subalgebra of $\mathfrak{A}$ for every $\theta_1 \in \mathfrak{A}$.

The proof is immediate.

Theorem 4.1 (First Isomorphism Theory, also see [3])

If θ_1 and θ_2 are two congruence relations of $\mathfrak{A}$ not necessarily permutable and $S_a(\theta_1)$ is a subalgebra of $\mathfrak{A}$ for some $a \in \mathfrak{A}$ then

$$S_a(\theta_2 \cdot \theta_1)/\theta_2 \cong S_a(\theta_1)/\theta_1\theta_2$$

Proof.

The homomorphic mapping θ_2^* of $S_a(\theta_1)$ to $S_a(\theta_2 \cdot \theta_1)/\theta_2$ is "onto", since if $x^{\theta_2 *} \in S_a(\theta_2 \cdot \theta_1)/\theta_2$, where $x \in S(\theta_2 \cdot \theta_1)$ we have $x\theta_2 x'\theta_1 a$ for some $x' \in \mathfrak{A}$. But this implies $x' \in S_a(\theta_1)$ and $x'^{\theta_2 *} = x^{\theta_2 *}$. Furthermore the congruence relations induced by θ_2 and $\theta_1\theta_2$ in $S_a(\theta_1)$ are the same, hence we have

$$S_a(\theta_2 \cdot \theta_1)/\theta_2 \cong S_a(\theta_1)/\theta_1\theta_2.$$

Remark. It follows immediately from § 3 that if θ_1 and θ_2 are permutable and $\mathfrak{A}$ has a selected one-element subalgebra 1, that we obtain $\theta_1 + \theta_2/\theta_2 \cong \theta_1/\theta_1\theta_2$ [3].

If θ and φ are any two congruence relations of $\mathfrak{A}$, $\varphi \geqslant \theta$, then it is clear that the residue classes of $\mathfrak{A}$ modulo θ are contained in the residue classes of $\mathfrak{A}$ modulo φ, hence φ determines in $\mathfrak{A}_\theta$ an equivalence relation $\bar{\varphi}$ which obviously is a congruence relation defined by

$$x^{\theta *} \equiv y^{\theta *} (\mathrm{mod}\ \bar{\varphi}) \text{ if and only if } x \equiv y (\mathrm{mod}\ \varphi).$$

The correspondence $\varphi \to \bar{\varphi}\ (\varphi \geqslant \theta)$ is one-one and clearly $\varphi_1 \leqslant \varphi_2$ if and only if $\bar{\varphi}_1 \leqslant \bar{\varphi}_2$. Thus we have

Theorem 4.2 (Second Isomorphism Theorem, also see [3], ix,Ex.2(a))

(i) For any $\theta \in C[\mathfrak{A}]$ the sublattice $[\theta, 1]$ of congruence relations of $\mathfrak{A}$ is isomorphic with the lattice $C[\mathfrak{A}_\theta]$ of congruence relations of $\mathfrak{A}_\theta$.

(ii) If $\varphi \geqslant \theta$ then $\mathfrak{A}_\varphi \cong (\mathfrak{A}_\theta)_{\bar{\varphi}}$.

We infer from the preceding theorem.

Theorem 4.3

If θ is a congruence relation of $\mathfrak{A}$ then the mapping $\varphi \rightarrow \bar{\varphi} = \overline{\varphi + \theta}$ is a complete sum-homomorphic mapping of $C[\mathfrak{A}]$ onto $C[\mathfrak{A}_\theta]$ (a complete sum-homomorphic mapping is a mapping preserving sums of arbitrary subsets).

Proof.

The proof is immediate since for every set $\{\varphi_\alpha\}$, $\alpha \in A$ of congruence relations of $\mathfrak{A}$ we have

$$\overline{\sum_{\alpha \in A} \varphi_\alpha} = \overline{\sum_{\alpha \in A} \varphi_\alpha + \theta} = \overline{\sum_{\alpha \in A} (\varphi_\alpha + \theta)} = \sum_{\alpha \in A} \left(\overline{\varphi_\alpha + \theta}\right) = \sum_{\alpha \in A} \bar{\varphi}_\alpha .$$

If $\varphi \geqslant \theta$ then by the mapping θ^*, every residue class of $\mathfrak{A}$ modulo φ is mapped onto the corresponding residue class of $\mathfrak{A}_\theta$ modulo $\bar{\varphi}$. If φ is an arbitrary congruence relation of $\mathfrak{A}$ not necessarily $\geqslant \theta$ then any residue class of $\mathfrak{A}$ modulo φ need not be mapped onto some residue class of $\mathfrak{A}_\theta$ modulo some congruence relation of $\mathfrak{A}_\theta$. However we can prove the following theorem.

Theorem 4.4

If θ and φ are any two permutable congruence relations of $\mathfrak{A}$ then by the mapping θ^* every residue class of $\mathfrak{A}$ modulo φ is mapped onto a residue class of $\mathfrak{A}_\theta$ modulo $\overline{\varphi + \theta}$.

Proof.

We shall prove that the residue class of $\mathfrak{A}$ modulo φ consisting of all the elements x for which $x \equiv a (\mathrm{mod}\, \varphi)$ is mapped into the residue class of $\mathfrak{A}_\theta$ modulo $\overline{\varphi + \theta}$, consisting of all the elements of $\mathfrak{A}_\theta$ congruent with $a^{\theta*}$ modulo $\overline{\varphi + \theta}$ and that this mapping is "onto". Indeed if $x\varphi a$ then $x(\varphi + \theta)a$. Now suppose that $x^{\theta*}(\overline{\varphi + \theta})a^{\theta*}$ then we have $x(\varphi + \theta)a$ and thus $a\varphi x'\theta z$ for some $x' \in \mathfrak{A}$ hence x' satisfies $x'\varphi a$ and $x'^{\theta*} = x^{\theta*}$

Theorem 4.5 (Lemma of Zassenhaus, also see [8])

If $\mathfrak{A}$ is an algebra with a selected one-element subalgebra 1 any two congruence relations are permutable then for any set of congruence relations θ_1, θ_2, φ_1 and φ_2 for which $\varphi_2 \leqslant \varphi_1$ and $\theta_2 \leqslant \theta_1$ we have

$$\varphi_1\theta_1 + \theta_2/\theta_2 + \varphi_2\theta_1 \cong \theta_1\varphi_1 + \varphi_2/\varphi_2 + \theta_2\varphi_1$$

Proof.

According to Theorem 4.1 and postulate (A) we have

$$\theta_1\varphi_1 + \theta_2/\theta_2 + \varphi_2\theta_1 \cong \theta_1\varphi_1 + \theta_2 + \varphi_2\theta_1/\theta_2 + \varphi_2\theta_1 \cong \theta_1\varphi_1/\theta_1\varphi_1(\theta_2 + \varphi_2\theta_1) \cong$$
$$\cong \theta_1\varphi_1/\theta_2\varphi_1 + \varphi_2\theta_1.$$

Similarly $\varphi_1\theta_1 + \varphi_2/\varphi_2 + \theta_2\varphi_1 \cong \varphi_1\theta_1/\varphi_2\theta_1 + \theta_2\varphi_1$ completing the proof.

(To be continued)